Open-Access-Compatibility Security Layer for Enhanced Protection Data Transmission

Todd Mander, Farhad Nabhani
University of Teesside, U.K.

Lin Wang, Richard Cheung
Ryerson University, Canada

Abstract — **Ongoing power system automaton and open access imposed by new government deregulations aggravate cyber-vulnerability of utility computer networks. This paper proposes an open-access-compatibility (OAC) security layer, installed beneath the data-link layer of the popular utility network protocol DNP3, to enhance data transmission security for utilities with open access capabilities. The OAC security is designed as an extension for a Canadian utility integrated P&C system innovation. The OAC security increases interactions with DNP3 data-link layer to enhance utility network security that is especially important for time-data-critical transmissions of protection information. The OAC security does not alter existing DNP3 specification to maintain interoperability for devices not using OAC. The OAC security uses two independent encryptions, one for exchanging security keys and one for transmitting data, to minimize time required for security operations. The OAC security relaxes authentication requirements to reduce transmission overheads and increase efficiency.**

Index Terms--**Computer networks, Computer network management, Computer network security, Power system communication, Power system security, Protocols, Security.**

I. Introduction

THIS paper proposes an open-access-compatibility (OAC) security layer for DNP3, a popular North American utility computer network protocol [1], providing confidentiality and authentication. The OAC security layer is designed to operate beneath the data-link layer of DNP3 but to avoid alterations to the existing DNP3 specification. The OAC security layer optimizes the data transmission security design by utilizing the existing DNP3 protocol stack to provide the required communication capability. The OAC security layer is derived from the cyber-security for DNP3 previously presented in [2] based on Pretty Good Privacy (PGP) [3][4]. However the transmissions of time-critical protection data could be delayed unnecessarily by the previously presented PGP-based security.

There are broad demands for power system utilities to adopt cyber-security [5]-[8], especially for the recent power-system operating environment with increased automation and government-imposed open access. The ongoing power system automation increases the number of devices connected in the utility computer network to enhance the power system operations, but this may create vulnerable locations from which the utility can be attacked. For example, the use of networked smart meters in the distribution system can facilitate various functions of metering such as recording time and attribute of electricity use, but the networked meters could produce security cracks for cyber-attacks. The power system automation also increases the use of devices with sophisticated communication capabilities such as exchanging data amongst themselves and with devices of external networks that can facilitate power system operations. However, increased data exchanges with devices of external networks in a peer-to-peer (P2P) networking could aggravate the opportunities for cyber-attackers to manipulate data that may cause power system devices malfunction or even failure.

Access to utility networks from external networks for electricity generation and trading transactions, due to government-imposed open access requirements, increases the number of users who are allowed to access the utility network through the Internet where not long ago, only trained utility staff had access to the utility network. This has considerably aggravated the risks into proper power system operations. For example, a cyber-attacker, through a compromised external access to the utility network, may send multiple DNP3 "stop" application function codes to strategic power system locations that could cause a wide-area blackout [9]. Previously no specific security was required for DNP3 since only a small number of trained staff had access to the utility network. Due to recent power system open-access operations, DNP3 has to have certain security measures such as encryption and authentication. Currently DNP3 does not specify data transmission security, except when it is used over TCP/IP that could cause cyber-security vulnerabilities for utility networks using DNP3 [10]-[13]. Plans for implementing authentication security for DNP3 has recently been proposed [14].

This paper presents the OAC security layer with open access compatibility for DNP3 using specific encryption and authentication without the need of altering the existing DNP3 specification. The OAC security layer is designed to be located beneath the DNP3 data-link layer. This security provides increased transparency to the DNP3 protocol stack with no change to the existing DNP3 specification. This security layer is designed to be interoperable with existing DNP3 devices of not using the OAC security. This permits a smooth phase-in for the OAC security layer implementation, as a smooth transition is usually required for live power systems. In addition, this security layer utilizes the communication capability of the DNP3 protocol stack for simplifying the security operations, i.e. the OAC security

T. Mander and F. Nabhani are with University of Teesside, U.K.
L. Wang and R. Cheung are with Ryerson University, Canada.

1-4244-1298-6/07/$25.00 ©2007 IEEE.

layer does not need to implement fragmentation, as otherwise it would be required for TLS [12].

The cyber-security for DNP3 was previously proposed to use PGP as a basis by the authors [2]. The cyber-security operated in two modes, one for public key cryptography (PGP-based security mode) and one for symmetric cryptography (symmetric-only security mode). The PGP-based security mode was used as a symmetric key exchange mechanism in which the symmetric key and authentication information was appended onto the DNP3 frame. However, the use of the PGP-based security for protection data would delay the data transmission unacceptably for proper power system protecting operations, because the PGP-based security mode is much time intensive than the symmetric-only cipher mode. Since the cyber-security of [2] was transparent to DNP3, there was no coordination between the cyber-security and the DNP3 protocol stack. Instead, the cyber-security of [2] could reduce potentials of delaying time-critical data by minimizing the use of the PGP-based security.

This paper proposes an enhancement to the cyber-security of [2] by ensuring that time-critical transmissions of protection or control data are not delayed by the public key cryptography. The OAC security layer proposed in this paper provides a security enhancement against replay attacks and increases the number of cyber-security features. The OAC security is capable of implementing secure communications for wide-areas, such as with the two-level hierarchical controller structure used for power system stability [15].

II. Encryption and Authentication

Encryption and authentication are the security measures for the development of the OAC security layer in this paper. Encryption provides confidentiality while authentication provides data transmission integrity. Without confidentiality, attackers could read the data passed between devices within the network. For example, a cyber-attacker could read a password used for DNP3 file transfers [9], and use that password to download files from a device or alter files on that device. Encryption can use either symmetric ciphers (single key cryptography) or asymmetric ciphers (public key cryptography). The symmetric ciphers are much fast in comparison to asymmetric ciphers and therefore are more suitable for the real-time security operations. However, the symmetric key ciphers do not have the authentication capability of the asymmetric ciphers and keys are difficult to exchange securely. Therefore, there are cipher schemes in which a hybrid approach is taken, such as with PGP where symmetric encryption is used for the data and asymmetric encryption is used for a security header. The asymmetric ciphers may be used as a mechanism to securely exchange symmetric cipher keys such as was used with TLS [12] and Internet Protocol Security (IPsec) [13][16].

Without authentication, the destination processor could not determine the integrity of data transmissions. The data transmission integrity requires the integrity of the data and the integrity of the source device. The data integrity will indicate if the transmitted data has been manipulated. For example without the data integrity, a cyber-attacker could alter a DNP3 stop application command from a single application to all devices by altering the qualifier code [9]. A message digest may be used to create the authentication, such as MD5 or SHA-1. However, it may still be possible for a cyber-attacker to manipulate a data-link frame while maintaining a correct value for the message digest. Security implementations, such as TLS and Ipsec, use HMAC that provides stronger authentication [12][13][17]. The source integrity authenticates the source device to the destination device. Without source integrity, an attacker could masquerade as another device that has permission to alter the destination device settings, such as stopping an application or causing the device to restart. The strong source integrity can be achieved through the non-repudiation capability of the asymmetric cryptography.

III. OAC Security Layer Encryption

A. Encryption Modes

Two encryptions of asymmetric and symmetric modes are considered in the design of the OAC security layer proposed in this paper. The asymmetric mode is used to securely exchange symmetric cipher keys between two devices while the symmetric mode is used for the encryption of the typical DNP3 data transmissions such as protection, control, and monitoring data. The two modes are basically independent of each other except for the asymmetric mode being used to update the symmetric mode's cipher key. Each DNP3 peer connection has its own asymmetric and symmetric modes that they are independent from other peer connections. Therefore each connection has its own set of asymmetric keys (source private and public keys, and destination public key) that are only valid for that connection plus the symmetric mode symmetric cipher key that is only valid for data transmissions to a particular destination.

Since asymmetric encryption is considerably slow in comparison to symmetric encryption, the asymmetric mode is used only for cipher key exchanges in a format similar to PGP. However, the asymmetric mode is unable to transmit empty frames containing the new symmetric cipher keys since the OAC security layer does not introduce any further communication capability to DNP3, but relies on the current DNP3 communication capability. Therefore, the asymmetric mode must use a DNP3 data-link layer frame to communicate the new symmetric cipher keys. For example, if the asymmetric mode data transmission was corrupted during transmission, the OAC security layer does not have the communication capability to detect and handle this situation. However, the DNP3 protocol layers would have the time-out timers to determine if a data transmission has not been responded and have the capability to retransmit the data.

The asymmetric mode cannot be used with the application layer message fragments, since this would delay transmissions of time-critical protection and control data, as well as non-time-critical monitoring data. However, the data-link layer function codes link status request and the responding link status can be used for the asymmetric mode data transmissions since they do not convey typical DNP3

protection, control, and monitoring data [18]. The link status request is transmitted from a network master or an outstation as a greeting message confirming that the link is still responding. The destination for the link status request responds with a link status message, confirming that the link is still working. Importantly, the link status request and the link status function code data transmissions do not contain important state information such as the transport layer or application layer sequence numbers. As a consequence, the asymmetric mode is not under a time-constraint in which to process and transmit the data-link frame containing these function codes. The asymmetric mode therefore does not interfere with processing and transmission of time-critical protection data using the symmetric mode.

Using the link status request function code data transmissions as the transport mechanism for the asymmetric mode requires increased interaction between the OAC security layer and the data-link layer. The asymmetric mode must be able to control the usage of the link status request function code, allowing the asymmetric mode to convey security when required. For example, the security layer cannot allow the data-link layer to begin a time-out timer until the data transmission had been processed and transmitted by the security layer [18]. The symmetric mode is used for all DNP3 data transmissions except for the link status request data transmissions. Therefore there is minimal processing and overhead for the control, protection, and monitoring data. Since there is one symmetric cipher key per link direction that is independent of each other, i.e. cipher key x used from the master to the outstation and cipher key y from the outstation to the master, the mechanism for exchanging symmetric ciphers keys is minimized. The OAC security layer does not dictate the cipher or cipher key size to be used for the symmetric operations, which is dependent on the desired security levels by the user.

B. Asymmetric Mode

There are two states for the asymmetric mode: active and inactive, as shown in Fig.1. The asymmetric mode is in the active state when it is transmitting symmetric cipher keys to the destination node. When the asymmetric mode is in the inactive state, it is not transmitting any data.

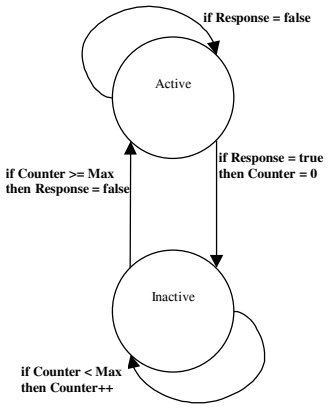

Fig. 1. Asymmetric mode state machine

In Fig.1, the asymmetric mode remains in the active state until it receives a link status response from the destination device. When the link status response to the link status request is received the state machine enters the inactive state. The state machine relies on the DNP request-response operations for the link status request function code. Once the DNP3 data-link layer has entered a link status wait state, it will remain in that state until it receives a response from the destination, or until the number of retries has exceeded the specified limit [18]. If the source device receives a link status function code response from the destination, the destination was therefore able to decrypt the data transmission correctly and receive the new symmetric cipher key. At this point, the transmitted symmetric key becomes the new cipher key used for the symmetric mode.

Once the asymmetric mode has entered the inactive state, it will remain in the inactive state for a specified number of data transmissions to the destination device. The specified number of data transmissions is a defined parameter for a particular peer connection and depends on the security confidence level for a particular link. Data transmissions occurring within a facility LAN would transition into the asymmetric encryption state rarely to replace the symmetric cipher keys since security risks are lower. Long-distance links between devices would have more exposure to cyber-attackers and would therefore have the symmetric cipher keys for that connection replaced more frequently.

The asymmetric mode active state operations are completed in three stages: symmetric encryption, frame authentication, and asymmetric encryption.

Stage 1: Symmetric Encryption

The symmetric encryption coverage of the data-link layer frame header is limited due to DNP3 P2P capabilities. The P2P networking requires that the source address field be transmitted in the clear (unencrypted) in order to allow the destination device to use the source address to look-up the cipher keys used for the connection. Since the source address cannot be encrypted, all header fields prior to the source address field cannot be encrypted either. The symmetric encryption can therefore only be applied to the Cyclic Redundancy Check (CRC) field in the data-link layer header block, as shown in Fig.2. This figure shows that the start (Start), length (Len), control (Ctrl), destination address (Dest), and source address (Source) header fields are in the clear while the CRC field is encrypted. Fig.2 also shows the optional authentication data block, discussed in Section IV for the authentication modes, that is appended onto the data-link layer frame that is also encrypted.

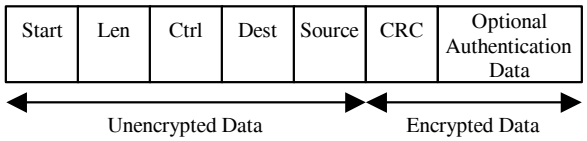

Fig. 2. Symmetric encryption of the DNP3 data-link layer frame for the asymmetric mode active state.

Stage 2: Frame Authentication

Typically the message authentication may be calculated only for the data encrypted by the symmetric cipher. However since most of the data-link layer header is in the clear, the message authentication must include the entire data-link

frame. If the authentication were not extended to the entire frame, attackers would be able to alter the header, such as the function codes causing errors, i.e. altering an ACK to a NACK, without being detected by the OAC security layer. Importantly, the asymmetric encryption mode uses the more secure encrypt-then-authenticate operation. The OAC security layer does not place constraints on the message authentication, although HMAC provides better authentication than simply using a message digest. The message digest coverage is shown in Fig. 3. The encrypted data consists of the header block CRC and possibly authentication data that is discussed in Section IV.

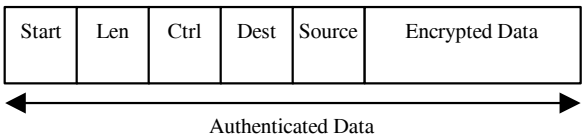

Fig. 3. Authentication coverage of encrypted DNP3 data-link layer frame for the asymmetric mode active state.

Stage 3 Asymmetric Encryption:

The asymmetric encryption operations firstly create a security header which is then encrypted using the asymmetric ciphers. The encrypted security header is then placed into the data-link layer frame. Fig. 4 shows the security header for the asymmetric mode.

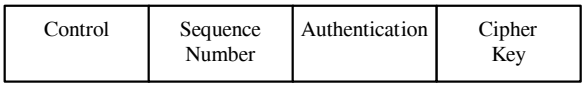

Fig. 4. Asymmetric mode security header.

The security header is composed of the following fields: control, sequence number, authentication, and cipher key.

Control: This field provides parameters to the OAC security layer for handling received data transmissions. The control field is shown in Fig.5 with the following fields: use key, authentication mode, and random padding. The use key field indicates if the received asymmetric mode frame's symmetric cipher key is to be used to replace the current symmetric cipher key. Otherwise the frame is used for conveying authentication mode information discussed in Section IV, which is indicated by the authentication mode field. The random padding is used for the interoperability operations discussed in Section V.

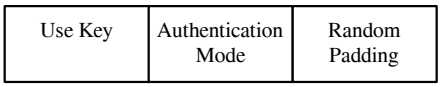

Fig. 5. Security header control field options.

Sequence number: used to provide security against replay attacks. DNP3 has inherent security against replay attacks due to the transport layer and application layer sequence numbers. If the received data transmission does not have the expected sequence numbers, the data will be discarded. Since the transport layer and the application layer have different sizes for the sequence number space [9],[19], having a data transmission that matches both sets of sequence numbers is less likely. However, the asymmetric mode itself is vulnerable to replay attacks without the sequence number since an attacker could cause the destination to accept new symmetric cipher keys. The sequence numbers and the symmetric mode provide security against this type of replay attack.

Authentication: contains the authentication generated from the encrypted data-link layer frame in stage 2. This field is variable depending on the type of message authentication used.

Cipher key: provides the symmetric cipher key used on the data from stage 1. If the control field's use key parameter is set, the cipher key field also provides the new symmetric cipher for the symmetric mode operations.

Once the security header has been generated and encrypted using the asymmetric cipher keys, the security header is placed into the data-link frame shown in Fig. 6. The security header is inserted into the data-link layer header after the start field since the start field may be used in the physical layer as a frame delimiter.

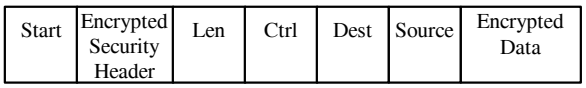

Fig. 6. Encrypted security header location within data-link layer frame.

C. Symmetric Mode

The symmetric mode is used for all DNP3 data transmissions except for the link status request and link status function codes data transmissions. The symmetric mode data transmissions to the destination are not delayed by the asymmetric mode operations if the data-link layer is not in the link status request states. However, once the data-link layer has entered the states associated with the link status request, further symmetric mode data transmissions would not be possible until a link status response is received [18]. Since decryption of the asymmetric mode data transmissions are time-intensive, time-critical data transmissions would be unduly delayed by this state condition. Therefore in order to remedy this condition, where time-critical data would be delayed unduly, further implementation changes are required to the DNP3 data-link layer by allowing user data to be transmitted and received while in this state.

Since the symmetric mode is independent on each side of the link, the symmetric key states required for the symmetric mode are simplified. For data transmissions from a device to the destination the current symmetric key is always used since it will only be updated by the asymmetric mode when it becomes valid to the destination (the active to inactive transition shown in Fig. 1). However, the destination uses two symmetric mode states for received data transmissions: current key and new key. The current key state is used for the symmetric mode decryption operations and contains the current valid symmetric key. The new key state contains the next symmetric cipher key that will be valid, and which was obtained from the last received asymmetric mode data transmission used to update the symmetric key. Due to the time-delays associated with the request-response operations of the asymmetric mode, and possibly due to transmission errors, it is not possible to precisely determine when the new key will be used by the source to the destination, requiring the symmetric encryption mode states at the destination shown in

Fig. 7 which is used to determine which symmetric key is to be used on the received data transmissions.

In Fig. 7, the symmetric mode remains in the current key state until the decryption operations using the current symmetric cipher key detects a transmission error, which is determined from the header CRC value. If a transmission error is detected, the symmetric mode will transition to the new key state. The data transmission will then be decrypted using the new symmetric cipher key from the last correctly received asymmetric mode data transmission. If a data transmission error is still detected, the symmetric mode will transition back to the current key state without any modifications to the states. This case represents a corrupted data transmission. If no data transmission errors are detected with the use of the new symmetric cipher key, the symmetric mode transitions back to the current key state, setting the new cipher key as the current cipher key.

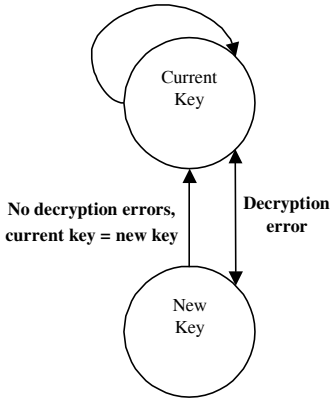

Fig. 7. Symmetric mode states at the destination.

The symmetric encryption operations are the same as those performed for the asymmetric mode. The symmetric encryption is performed on the CRC field in the header block and the user data blocks, shown in Fig. 8. The symmetric encryption does not include most of the data-link header since the source address must be in the clear due to the P2P networking. The symmetric mode authentication discussed in Section IV has the same coverage as the asymmetric mode shown in Fig.3. The symmetric encryption uses the more secure encrypt-then-authenticate operation than what was proposed in [2]. The symmetric mode does not insert the authentication into the data-link frame, discussed in Section IV, in order to increase the transmission efficiency of the DNP3 control, protection, and monitoring data transmissions.

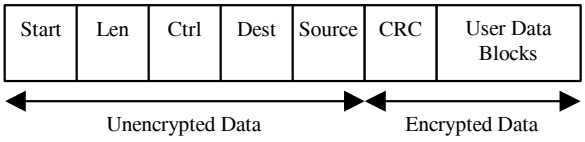

Fig. 8. Symmetric mode encryption coverage

IV. OAC Security Layer Authentication

A. Authentication Modes

Authentication operations generate additional data that is appended onto data transmissions. As a result, data takes longer to transmit, which may cause unacceptable delays in time-critical protection data transmissions, such as those dealing with wide-area power system stability discussed in [15]. Therefore in order to improve the efficiency of the OAC security layer, the symmetric mode does not include the frame authentication with its data transmissions. The addition of authentication to the asymmetric mode security header does not degrade the asymmetric mode transmission efficiency since the encrypted security header will be the same size regardless if the authentication data was included or not due to the larger block sizes used by the asymmetric ciphers.

The OAC security layer symmetric mode authentication is performed after the data has been encrypted. The authentication therefore uses the more desirable encrypt-then-authenticate for all data transmissions, which requires the authentication to be transmitted separately from the frame being authenticated in any case. The OAC security layer uses the trust-me-until-proven-otherwise format for the symmetric mode security. Since the symmetric encryption, which has the cipher keys properly authenticated using the asymmetric mode, and the user data block CRCs should provide sufficient authentication for most cases, including explicit frame authentication within the symmetric mode data transmission using HMAC or message digest is redundant. The OAC security layer therefore provides two authentication modes for the symmetric mode that are used to provide authentication between the source and destination devices, which are: standard and enhanced modes. The standard mode, which is discussed in the next subsection, provides flexibility and is used for limited bandwidth cases. The enhanced authentication mode requires higher bandwidth but provides stronger security and is discussed in the subsection following the standard authentication mode subsection.

B. Standard Authentication Mode

In the standard authentication mode, the authentications generated by the symmetric mode are stored as DNP3 data that can be retrieved by the destination device to confirm the integrity of the data as necessary. The authentications are generated on a data-link layer frame basis. Therefore, the transport layer sequence numbers [19] are used to reference the authentications. However, since the transport layer sequence number space is very small, with only 64 numbers [19], the authentications have to be accessed within a very short period of time before they are over written by the new authentication values. Transmitting all of the authentications referenced by the transport layer sequence number may be difficult for devices with low bandwidths depending on the size of the message authentication used. Since the OAC security layer assumes that the data integrity is high, even without the authentication being included within the data transmission, not all authentications would be required to confirm the ongoing integrity of data transmissions. Instead, a random sampling of the authentications can be taken by the destination to confirm the overall integrity of the data transmissions, with the sample size dependent on the bandwidth constraints for transmitting the authentications.

C. Enhanced Authentication Mode

In the enhanced authentication mode, the authentications generated by the symmetric mode are transmitted with the

asymmetric mode data transmissions. Using the asymmetric mode as the transport mechanism for the symmetric authentications increases the symmetric mode authentication security. The asymmetric mode operations will include the authentication of the encrypted authentications in the security header, thereby providing full data integrity for that data transmission as well as non-repudiation. Although the enhanced authentication mode provides increased security for transmitting the symmetric mode authentications, it requires increased processing and transmission performance. With the symmetric authentication values referenced by the transport layer sequence numbers, the sequence space is very small with only 64 numbers [19]. Therefore, the asymmetric mode has to process and transmit the authentications within this time period before the authentication numbers are over-written as was the case for the standard authentication mode.

The small sequence space for the transport layer sequence numbers will require the generation of asymmetric mode data transmissions on a more frequent basis than what would typically be required for the replacement of the symmetric cipher keys. Therefore, the key used parameter of the security header control field can be used to indicate if the current symmetric encryption key should be replaced with the currently received symmetric cipher key or if it was used for the current data transmission only. The enhanced authentication mode requires that the OAC security layer header control field parameter authentication mode be set. This indicates that the data following the header CRC are a list of symmetric mode authentications.

As with the standard authentication mode, the enhanced authentication mode only uses a random sampling of symmetric authentications to minimize the amount of data being transmitted. Unlike the standard authentication mode, the enhanced authentication mode does not provide error control and recovery. The asymmetric mode generates an entirely new link status request data transmission with a new symmetric encryption key. Therefore, new asymmetric mode data transmissions would contain an entirely different sampling of symmetric mode authentications each time a new data transmission was generated.

V. Interoperability

An important requirement for the OAC security layer is interoperability between devices that use and do not use the OAC security layer. In addition, the OAC security layer must be able to detect which encryption security mode is being used for received data transmissions. The interoperability operations are divided into two steps: determination of asymmetric mode and determination of symmetric mode.

A. Determination of the Asymmetric Mode

The determination if the asymmetric mode has been used on the data transmission can be obtained from calculating the CRC-16 for the first 8 octets of the data-link layer frame header. If the calculated CRC-16 is equal to the received data-link layer header CRC-16 value in location octet 9 and 10, then asymmetric encryption was not used on the frame. If the CRC values do not match then either the asymmetric mode was used or a data transmission error has occurred.

Determining if a data transmission error has occurred can be decided from applying the asymmetric mode operations and using the message authentication to check for errors. However, this is a time consuming process, especially for noisy environments where there would be a greater tendency towards transmission errors. Therefore, a more efficient determination of the asymmetric mode can be used based on the size of the data transmission. Since the asymmetric mode increases the size of the data transmission close to the maximum size of a DNP3 data-link layer frame, the enhanced authentication mode will increase the frame size beyond the maximum size. Therefore frames greater than the maximum size used the OAC security layer. If the standard authentication mode is used, padding can be added into the data-link frame to increase its size to value greater than the maximum data-link layer frame size. The padding is added after the asymmetric operations and appended after the security header. The padding is removed by the destination after it has determined that the standard authentication mode has been used from the authentication mode parameter in the OAC security layer header control field.

This more efficient check determines if security has been used on the frame, but not which security mode. The symmetric mode may also increase the frame size beyond the maximum DNP3 data-link frame size. Therefore, the amount of authentications added by the enhanced authentication mode or the amount of padding added into the frame for the standard authentication mode have to exceed the maximum frame size increase by the symmetric mode as well. Otherwise, the asymmetric mode authentication will have to be used to determine if a data transmission error occurred. It is possible for the encrypted security header to create matching calculated and received CRC values for the asymmetric mode encryption operations. Therefore, the source device must test for this condition. If matching CRC values are discovered for an asymmetric mode data transmission, the random padding parameter in the security header control field is altered to remove this condition. This is a performance improvement over [2] which has the symmetric key altered, and hence the authentication as well, to correct this condition.

B. Determination of the Symmetric Mode

Determining if the symmetric mode has been used can be obtained from calculating the CRC-16 for the header and matching it to the received CRC-16, as discussed for determining the asymmetric mode. If the CRC is match, then the source address can be used to determine if the OAC security is used for the peer connection. If encryption keys exist for the connection, then security was used and therefore the frame has used the symmetric mode. Otherwise, no security was used on the frame, and it can be sent directly to the DNP3 data-link layer. The OAC security layer requires that once security is used for a peer connection, it will be always used. Therefore, if a data transmission is received on a connection that uses the OAC security but the frame has not

used the OAC security, it will be rendered indecipherable by the OAC security layer to the data-link layer of DNP3 since the symmetric mode will be applied regardless. This increases the security against manufactured frames sent into the DNP3 network for a connection that is using the OAC security.

VI. Conclusion

The ongoing power system utility automaton and open-access under government imposed deregulation is increasing the cyber-vulnerabilities of utility computer networks. This paper has proposed the OAC security layer with open-access compatibility, located beneath the data-link layer, to provide the popular utility network protocol DNP3 with strong data transmission security under open access deregulated power system environment. The OAC security layer does not require alterations to the existing DNP3 specification, in order to provide interoperability capability with devices of not using the OAC security. The OAC security layer requires increased interaction with the DNP3 data-link layer for controlling the security operations. The increased interaction with the data-link layer enhances the performance of the OAC security layer, which is especially important for the transmission of time-critical protection data.

The OAC security was originally designed for increasing the reliability level for time-data-critical transmissions of protection information, as an extension for a Canadian utility integrated P&C system innovation. This paper has described the OAC security design. Two encryptions of asymmetric and symmetric modes have been considered in the design of the OAC security layer. The asymmetric mode, which is used to exchange symmetric cipher keys, is independent of the symmetric mode, which is used for control, protection, and monitoring data transmissions. The asymmetric mode operations are therefore unable to cause data transmission delays for the data using the symmetric mode. The symmetric mode therefore minimizes the OAC security layer's impact on the data transmission timing for time-critical protection data. To further enhance the performance of the OAC security layer, the symmetric mode authentication is omitted from the data transmissions. The authentications are either accessed from the device as DNP3 data or appended onto the asymmetric mode data transmissions. With this trust-me-until-proven otherwise format, the overhead of transmitting authentications with the symmetric mode data transmissions is eliminated, which can drastically increase the size of the frame. As a result, time-critical data transmissions are transmitted and received quicker by the DNP3 devices since there is less data being transmitted.

VII. References

[1] "The World Market for Substation Automation and Integration Programs in Electric Utilities: 2005-2007 Executive Summary North American Market," Newton-Evans Research Company, September 2005.

[2] T. Mander, L. Wang, R. Cheung, and F. Nabhani, "Adapting the Pretty Good Privacy Security Style to Power System Distributed Network Protocol," in *Proc. 2006 IEEE Large Engineering Systems Conference on Power Engineering (LESCOPE 2006) Conf.*, pp. 79-83.

[3] *RFC 1991: PGP Message Exchange Formats*, Internet Engineering Task Force (IETF), August 1996.

[4] P. R. Zimmermann, *The Official PGP User's Guide*, Cambridge: The MIT Press, 1997.

[5] "The National Strategy For The Physical Protection of Critical Infrastructures and Key Asset", U.S. Department of Homeland Security, February 2003, pp. 50-53.

[6] "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendation," U.S.-Canada Power System Outage Task Force, April 2004.

[7] M. Amin "Balancing Market Priorities with Security Issues", *IEEE Power & Energy Magazine,* July/August 2004. pp. 30-38.

[8] J. Kumagai "Nine Cautionary Tales", *IEEE Spectrum*, September 2006, vol. 43, no. 9, pp. 36-45.

[9] *DNP3 Specification Volume 2: Application Layer*, DNP User's Group, October 2005.

[10] *DNP3 Specification Volume 7: IP Networking*, DNP User's Group, December 2004.

[11] "Security Update", DNP User's Group, February 2006.

[12] *RFC 4346: The TLS Protocol Version 1.1*, Internet Engineering Task Force (IETF), April 2006.

[13] *RFC 4301: Security Architecture for the Internet*, Internet Engineering Task Force (IETF), December 2005.

[14] *DNP3 Technical Bulletin TB2005-003: Plans to Implement Authentication Security Draft*, DNP User's Group, November 2005.

[15] F. Okou, L. Dessaint, and O. Akhrif, "Power System Stability Enhancement Using a Wide-Area Signals Based Hierarchical Controller," *IEEE Transactions on Power Systems*, vol. 20, no. 3, August 2005, pp. 1465-1477.

[16] *RFC 4306: Internet Key Exchange (IKEv2) Protocol*, Internet Engineering Task Force (IETF), December 2005.

[17] *RFC 2104: HMAC: Keyed-Hashing for Message Authentication*, Internet Engineering Task Force (IETF), February 1997.

[18] *DNP3 Specification Volume 4: Data Link Layer*, DNP User's Group, December 2002.

[19] *DNP3 Specification Volume 3: Transport Function*, DNP User's Group, November 2002.

VIII. Biographies

Todd Mander received his B.Eng. degree from Ryerson University. He is currently working on his doctorate degree in power system computer networks at the University of Teesside through Ryerson University.

Farhad Nabhani has B.Sc., M.Sc., and Ph.D. degrees. He is a Reader and M.Sc. Course Leader at the University of Teesside.

Lin Wang received her B.Eng., M.Eng., and Ph.D. degrees from Huazhong University of Science and Technology, and was an Associate Professor at the same university. She is currently conducting research at Ryerson University.

Richard Cheung received his B.A.Sc., M.A.Sc., and Ph.D. degrees from the University of Toronto. He was a Research Engineer in Ontario Hydro. Currently he is a Professor at Ryerson University, and he is an active Power Engineering consultant and is the President of RC Power Conversions Inc.